Cryptography and Network Security

Syllabus:

UNIT I :

Classical Encryption Techniques Objectives:

The Objectives of this unit is to present an overview of the main concepts of cryptography, understand the threats & attacks, understand ethical hacking.

Introduction: Security attacks, services & mechanisms, Symmetric Cipher Model, Substitution Techniques, Transportation Techniques, Cyber threats and their defense(Phishing Defensive measures, web based attacks, SQL injection & Defense techniques)(TEXT BOOK 2), Buffer overflow & format string vulnerabilities, TCP session hijacking(ARP attacks, route table modification) UDP hijacking (man-in-the-middle attacks)(TEXT BOOK 3).

UNIT II:

Block Ciphers & Symmetric Key Cryptography Objectives:

The Objectives of this unit is to understand the difference between stream ciphers & block ciphers, present an overview of the Feistel Cipher and explain the encryption and decryption, present an overview of DES, Triple DES, Blowfish, IDEA.

Traditional Block Cipher Structure, DES, Block Cipher Design Principles, AES-Structure, Transformation functions, Key Expansion, Blowfish, CAST-128, IDEA, Block Cipher Modes of Operations.

UNIT III:

Number Theory & Asymmetric Key Cryptography Objectives: Presents the basic principles of public key cryptography, Distinct uses of public key cryptosystems.

Number Theory: Prime and Relatively Prime Numbers, Modular Arithmetic, Fermat's and Euler's Theorems, The Chinese Remainder theorem, Discrete logarithms.

Public Key Cryptography: Principles, public key cryptography algorithms, RSA Algorithms, Diffie Hellman Key Exchange, Elgamal encryption & decryption, Elliptic Curve Cryptography.

UNIT IV :

Cryptographic Hash Functions & Digital Signatures Objectives:

Present overview of the basic structure of cryptographic functions, Message Authentication Codes, Understand the operation of SHA-512, HMAC, Digital Signature.

Application of Cryptographic hash Functions, Requirements & Security, Secure Hash Algorithm, Message Authentication Functions, Requirements & Security, HMAC & CMAC. **Digital Signatures** NIST Digital Signature Algorithm.

Key management & distribution.

UNIT V:

User Authentication, Transport Layer Security & Email Security Objectives:

Present an overview of techniques for remote user authentication, Kerberos, Summarize Web Security threats and Web traffic security approaches, overview of SSL & TLS. Present an overview of electronic mail security.

User Authentication: Remote user authentication principles, Kerberos Transport Level Security: Web Security Requirements, Secure Socket Layer (SSL) and Transport Layer Security (TLS), Secure Shell(SSH).

Electronic Mail Security: Pretty Good Privacy (PGP) and S/MIME.

UNIT VI:

IP Security & Intrusion Detection Systems Objectives:

Provide an overview of IP Security, concept of security association, Intrusion Detection Techniques.

IP Security: IP Security Overview, IP Security Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations and Key Management.

Intrusion detection: Overview, Approaches for IDS/IPS, Signature based IDS, Host based IDS/IPS. (TEXT BOOK 2).

TEXT BOOKS:

1. Cryptography & Network Security: Principles and Practices, William Stallings, PEA, Sixth edition.
2. Introduction to Computer Networks & Cyber Security, Chwan Hwa Wu, J.David Irwin, CRC press
3. Hack Proofing your Network, Russell, Kaminsky, Forest Puppy, Wiley Dreamtech.

REFERENCE BOOKS:

1.Everyday Cryptography, Fundamental Principles & Applications, Keith Martin, Oxford
2.Network Security & Cryptography, Bernard Menezes, Cengage,2010

UML & DESIGN PATTERNS

Syllabus:

Unit 1: Introduction : Introduction to OOAD; typical activities / workflows / disciplines in OOAD, Introduction to iterative development and the Unified Process, Introduction to UML; mapping disciplines to UML artifacts,
Introduction to Design Patterns - goals of a good design, introducing a case study & MVC architecture

Unit 2: Inception: Artifacts in inception, Understanding requirements - the FURPS model, Understanding Use case model - introduction, use case types and formats, Writing use cases - goals and scope of a use case, elements/sections of a use case, Use case diagrams, Use cases in the UP context and UP artifacts, Identifying additional requirements, Writing requirements for the case study in the use case model

Unit 3: Elaboration: System sequence diagrams for use case model, Domain model : identifying concepts, adding associations, adding attributes, Interaction Diagrams, Introduction to GRASP design Patterns ,Design Model: Usecase realizations with GRASP patterns, Design Class diagrams in each MVC layer Mapping Design to Code, Design class diagrams for case study and skeleton code

Unit 4: More Design Patterns: Fabrication, Indirection, Singleton, Factory, Facade, Publish-Subscribe

Unit 5: More UML diagrams: State-Chart diagrams, Activity diagrams, Component Diagrams, Deployment diagrams, Object diagrams

Unit 6: Advanced concepts in OOAD: Use case relationships, Generalizations, domine model refinements, architecture, packaging model elements

TEXT BOOKS:

T1. 'Applying UML and patterns' by Craig larman,Pearson.
T2. 'Object oriented analysis & design with unified process' by Satzinger, Jackson & burd Cengage learning.
T3. 'UML Distilled' by Martin Fowler , Addison Wesley, 2003
T4. 'Software project management' by wlker royce, Pearson.
T5. 'The unified modeling language user guide' by Grady booch,James Rumbaugh,Ivar Jacobson.

REFERENCES:

R1. O'reilly ' s 'Head-First Design Patterns' by Eric Freeman et al, Oreillly
R2. UML 2 Toolkit, by Hans-Erik Eriksson, Magnus Penker, Brian Lyons, David Fado: WILE\' Dreamtech lndia. pvt.lid.

Mobile Computing

Syllabus:

UNIT I

Introduction: Mobile Communications, Mobile Computing – Paradigm, Promises/Novel Applications and Impediments and Architecture; Mobile and Handheld Devices, Limitations of Mobile and Handheld Devices.

GSM – Services, System Architecture, Radio Interfaces, Protocols, Localization, Calling, Handover, Security, New Data Services, GPRS.

UNIT –II

(Wireless) Medium Access Control (MAC) : Motivation for a specialized MAC (Hidden and exposed terminals, Near and far terminals), SDMA, FDMA, TDMA, CDMA, WirelessLAN/(IEEE 802.11)

UNIT –III

Mobile Network Layer: IP and Mobile IP Network Layers, Packet Delivery and Handover Management, Location Management, Registration, Tunneling and Encapsulation, Route Optimization, DHCP.

UNIT –IV

Mobile Transport Layer: Conventional TCP/IP Protocols, Indirect TCP, Snooping TCP, Mobile TCP, Other Transport Layer Protocols for Mobile Networks.

Database Issues: Database Hoarding & Caching Techniques, Client-Server Computing & Adaptation, Transactional Models, Query processing, Data Recovery Process & QoS Issues.

UNIT V

Data Dissemination and Synchronization : Communications Asymmetry, Classification of Data Delivery Mechanisms, Data Dissemination, Broadcast Models, Selective Tuning and Indexing Methods, Data Synchronization – Introduction, Software, and Protocols.

UNIT VI

Mobile Ad hoc Networks (MANETs) : Introduction, Applications & Challenges of a MANET, Routing, Classification of Routing Algorithms, Algorithms such as DSR, AODV, DSDV, etc. , Mobile Agents, Service Discovery.

Protocols and Platforms for Mobile Computing : WAP, Bluetooth, XML, J2ME, JavaCard, PalmOS, Windows CE, SymbianOS, Linux for Mobile Devices, Android.

TEXT BOOKS:

1. Jochen Schiller, “Mobile Communications”, Addison-Wesley, Second Edition, 2009.
2. Raj Kamal, “Mobile Computing”, Oxford University Press, 2007, ISBN: 0195686772

REFERENCE BOOKS:

1. ASOKE K TALUKDER, HASAN AHMED, ROOPA R YAVAGAL, “Mobile Computing, Technology Applications and Service Creation” Second Edition, Mc Graw Hill.
2. UWE Hansmann, Lother Merk, Martin S. Nocklous, Thomas Stober, “Principles of Mobile Computing,” Second Edition, Springer.

INFORMATION RETRIEVAL SYSTEMS

Syllabus:

UNIT I:

Introduction to Information Storage and Retrieval System: Introduction, Domain Analysis of IR systems and other types of Information Systems, IR System Evaluation.

Introduction to Data Structures and Algorithms related to information Retrieval: Basic Concepts, Data Structures ,Algorithms

UNIT II:

Inverted Files: Introduction, Structures used in Inverted Files, Building Inverted File using a sorted array, Modifications to Basic Techniques.

UNIT III:

Signature Files: Introduction, Concepts of Signature Files, Compression, Vertical Partitioning, Horizontal Partitioning

UNIT IV:

New Indices for Text: PAT Trees and PAT Arrays **:** Introduction , PAT Tree structure ,algorithms on the PAT Trees, Building PAT trees as PATRICA trees, PAT representation as arrays.

UNIT V:

Stemming Algorithms: Introduction, Types of Stemming Algorithms, Experimental Evaluations of Stemming to Compress Inverted Files

UNIT VI:

Thesaurus Construction: Introduction, Features of Thesauri, Thesaurus construction, Thesaurus construction from Texts, Merging existing Thesauri

TEXT BOOKS:

T1 Frakes, W.B., Ricardo Baeza - Yates: Information Retrieval Data Structures and Algorithms, Prentice Hall , 1992.

T2 Modern Information Retrieval by Yates Pearson Education.

T3 Information Storage & Retrieval By Robert Korfhage - John Wiley & Sons.

REFERENCES:

R1 Kowalski, Gerald, Mark T Maybury : Information Retrieval Systems: Theory and Implementation, Kluwer Academic Press, 1997.

R2 Information Retrieval Algorithms and Heuristics , 2ed, Springer.

Hadoop and BigData

Syllabus:

UNIT – I :

Data structures in Java: Linked List, Stacks, Queues, Sets, Maps; Generics: Generic classes and Type parameters, Implementing Generic Types, Generic Methods, Wrapper Classes, Concept of Serialization.

UNIT – II:

Working with Big Data: Google File System, Hadoop Distributed File System (HDFS) –Building blocks of Hadoop (Namenode, Datanode, Secondary Namenode, Job Tracker, TaskTracker), Introducing and Configuring Hadoop cluster (Local, Pseudo-distributed mode, Fully Distributed mode), Configuring XML files.

UNIT – III:

Writing MapReduce Programs: A Weather Dataset, Understanding Hadoop API for MapReduce Framework (Old and New), Basic programs of Hadoop Map Reduce: Driver code, Mapper code, Reducer code, RecordReader, Combiner, Partitioner.

UNIT – IV:

Hadoop I/O: The Writable Interface, WritableComparable and comparators, Writable Classes: Writable wrappers for Java primitives, Text, BytesWritable, NullWritable, ObjectWritable and GenericWritable, Writable collections, Implementing a Custom Writable: Implementing a RawComparator for speed, Custom comparators.

UNIT – V:

Pig: Hadoop Programming Made Easier Admiring the Pig Architecture, Going with the Pig Latin Application Flow, Working through the ABCs of Pig Latin, Evaluating Local and Distributed Modes of Running Pig Scripts, Checking out the Pig Script Interfaces, Scripting with Pig Latin.

UNIT – VI:

Applying Structure to Hadoop Data with Hive: Saying Hello to Hive, Seeing How the Hive is Put Together, Getting Started with Apache Hive, Examining the Hive Clients, Working with Hive Data Types, Creating and Managing Databases and Tables, Seeing How the Hive Data Manipulation Language Works, Querying and Analyzing Data.

TEXT BOOKS:

1. Big Java 4th Edition, Cay Horstmann, Wiley John Wiley & Sons, INC
2. Hadoop: The Definitive Guide by Tom White, 3rd Edition, O'reilly
3. Hadoop in Action by Chuck Lam, MANNING Publ.
4. Hadoop for Dummies by Dirk deRoos, Paul C.Zikopoulos, Roman B.Melnyk, Bruce Brown, Rafael Coss

REFERENCE BOOKS:

1. Hadoop in Practice by Alex Holmes, MANNING Publ.
2. Hadoop MapReduce Cookbook,Srinath Perera, Thilina Gunarathne

Software Links:

1. Hadoop:http://hadoop.apache.org/
2. Hive: https://cwiki.apache.org/confluence/display/Hive/Home

UML and Design Patterns Lab

Syllabus:

Week 1:

Familiarization with Rational Rose or Umbrello.

Week 2,3 & 4:

For each case study:

a) Identity and analyze events
b) Identity Use cases
c) Develop event table
d) Identity & analyze domain classes
e) Represent use cases and a domain class diagram using Rational Rose
f) Develop CRUD matrix to represent relationships between use cases and problem domain classes

Week 5 & 6:

For each case study:

a) Develop Use case diagrams
b) Develop elaborate Use case descriptions & scenarios
c) Develop prototypes (without functionality)
d) Develop system sequence diagrams

Week 7,8,9 & 10:

For each case study:

a) Develop high-level sequence diagrams for each use case
b) Identify MVC classes / objects for each use case
c) Develop Detailed Sequence Diagrams / Communication diagrams for each use case showing interactions among all the three-layer objects
d) Develop detailed design class model (use GRASP patterns for responsibility assignment)
e) Develop three-layer package diagrams for each case study

Week 11 & 12:

For each case study:

a) Develop Use case Packages
b) Develop component diagrams
c) Identify relationships between use cases and represent them
d) Refine domain class model by showing all the associations among classes

Week 13 onwards:
For each case study:
Develop sample diagrams for other UML diagrams – state chart diagrams, activity diagrams and deployment diagrams

Mobile Application Development Lab

Syllabus:

1. Write a J2MH program to show how to change the font size and colour.

2. Write a J2ME program which creates the following kind of menu.
    - cut
    - copy
    - past
    - delete
    - select all
    - unselect all

3. Create a J2ME menu which has the following options (Event Handling):
   cut - can be on/off
   copy - can be on/off
   paste - can be on/off
   delete - can be on/off
   select all - put all 4 options on
   unselect all - put all

4. Create a MIDP application, which draws a bar graph to the display. Data values can be given at int [] array.You can enter four data (integer) values to the input text field.

5. Create an MIDP application which examine, that a phone number,which a user has entered is in the given format (Input checking):
    - Areacodeshouldbeoneofthefollowing: 040,041,050,0400,044
    - There should 6-8 numbers in telephone number (+ area code)

6. Write a sample program to show how to make a SOCKET Connection from J2ME phone. This J2ME sample program shows how to how tomake a SOCKET Connection from a J2ME Phone. Many a times there is a need to connect backend HTTP server from the 2ME application. Show how to make a SOCKET connection from the phone to port 80.

7. Login to HTTP Server from a J2ME Program. This J2ME sample program shows how to display a simple LOGIN SCREEN on the J2ME phone and how to authenticate to a HTTP server. Many J2ME applications for security reasons require the authentication of
   the user. 'This free J2ME sample program, shows how a J2ME application can do authentication to the backend server. Note: Use Apache Tomcat Server as Web Server and MySQL as Database Server.

8. The following should be carried out with respect to the given set of application domains: (Assume that the Server is connected to the well-maintained database of the given domain. Mobile Client is to be connected to the Server and fetch the required data value/information)
    - Students Marks Enquiry
    - Town/City Movie Enquiry
    - Railway/Road/Air (For example PNR) Enquiry/Status
    - Sports (say, Cricket) Update
    - Town/City Weather Update

    Public Exams (say Intermediate or SSC)/ Entrance (Say EAMCET) Results Enquiry

    Divide Student into Batches and suggest them to design database according to their domains and render information according the requests.

9. Write an Android application program that displays Hello World using Terminal.

10. Write an Android application program that displays Hello World using Eclipse.

11. Write an Android application program that accepts a name from the user and displays the hello name to the user in response as output using Eclipse.

12. Write an Android application program that demonstrates the following:
    (i) Linear Layout
    (ii)Relative Layout
    (iii)Table Layout
    (iv) Grid View layout
13. Write an Android application program that converts the temperature in Celsius to Fahrenheit.

14. Write an Android application program that demonstrates intent in mobile application development.

Software Engineering Lab

Syllabus:

Take any real time problem and do the following experiments.

1. Do the Requirement Analysis and Prepare SRS
2. Using COCOMO model estimate effort.
3. Calculate effort using FP oriented estimation model.
4. Analyze the Risk related to the project and prepare RMMM plan.
5. Develop Time-line chart and project table using PERT or CPM project scheduling methods.
6. Draw E-R diagrams, DFD, CFD and structured charts for the project.
7. Design of Test cases based on requirements and design.
8. Prepare FTR
9. Prepare Version control and change control for software configuration items.

Hadoop & BigData Lab

Syllabus:

Week 1,2:

1. Implement the following Data structures in Java
   a) Linked Lists b) Stacks c) Queues d) Set e) Map

Week 3, 4:

2. (i) Perform setting up and Installing Hadoop in its three operating modes:
   Standalone
   Pseudo distributed
   Fully distributed
   (ii) Use web based tools to monitor your Hadoop setup.

Week 5:

3. Implement the following file management tasks in Hadoop:
   - Adding files and directories.
   - Retrieving files.
   - Deleting files

   Hint: A typical Hadoop workflow creates data files (such as log files) elsewhere and copies them into HDFS using one of the above command line utilities.

Week 6:

4. Run a basic Word Count Map Reduce program to understand Map Reduce Paradigm.

Week 7:

5. Write a Map Reduce program that mines weather data. Weather sensors collecting data every hour at many locations across the globe gather a large volume of log data, which is a good candidate for analysis with MapReduce, since it is semi structured and record-oriented.

Week 8:

6. Implement Matrix Multiplication with Hadoop MapReduce

Week 9,10:

7. Install and Run Pig then write Pig Latin scripts to sort, group, join, project, and filter your data.

Week 11,12:

8. Install and Run Hive then use Hive to create, alter, and drop databases, tables, views, functions, and indexes.